REMARKS

This application has been reviewed in light of the Office Action dated November 10, 2003. Claims 1-18 are presented for examination, of which Claims 1, 10, and 18 are in independent form. The independent claims have been amended to define Applicant's invention more clearly, and Claims 4, 5, 8, and 13 have been amended as to formal matters. Favorable reconsideration is requested.

The Office Action states that Claims 1-16 and 18 are rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,608,786 (Gordon); and that Claim 17 is rejected under § 103(a) as being unpatentable over Gordon in view of U.S. Patent No. 5,521,719 (Yamada). Applicant respectfully traverses the rejections and submits that independent Claims 1, 10, and 18, together with the claims dependent therefrom, are not anticipated by Gordon for at least the following reasons.

An aspect of the present invention set forth in Claim 1 is directed to a communication apparatus connected to a communication network. The apparatus includes destination designating means, input means, facsimile communication means, encryption means, electronic-mail communication means, communication designating means, security designating means, and control means. The destination designating means is adapted to designate a destination apparatus, and the input means is adapted to input transmission information to be transmitted to the designated destination apparatus without using the communication network.

The facsimile communication means is adapted to transmit the inputted transmission information to a destination apparatus in accordance with facsimile communication

specifications. The encryption means is adapted to encrypt the inputted transmission information without using the communication network, that is, the transmission information is encrypted before being transmitted through the communication network to maintain confidentiality of the transmission information. The electronic-mail communication means is adapted to transmit the inputted transmission information or the encrypted transmission information to a destination apparatus in accordance with electronic-mail specifications.

The communication designating means is adapted to cause transmission of the transmission information by selecting either the facsimile communication means or the electronic-mail communication means. The security designating means is adapted to designate whether the transmission information is confidential or not according to an operation of a confidential button, which is used when confidentiality of the transmission information is to be maintained.

The control means is adapted to control the facsimile communication means, the encryption means, and the electronic-mail means. If the transmission information has been designated as being confidential by the security designating means, and when the facsimile communication means has been designated by the communication designating means, the control means controls the facsimile communication means to transmit the inputted transmission information to the destination apparatus by facsimile transmission through the communication network. If the transmission information has been designated as being confidential by the security designating means, and when the electronic-mail communication means has been designated by the communication designating means, the control means controls the electronic-

mail communication means to send the encrypted transmission information to the destination apparatus by electronic mail through the communication network.

One of the notable features of Claim 1 is that the security designating means is adapted to designate whether the transmission information is confidential or not according to an operation of a confidential button, which is used when confidentiality of the transmission information is to be maintained. If the transmission information is designated to be confidential, and depending on whether a facsimile communication or an electronic-mail communication is to be performed, the transmission information is encrypted prior to being transmitted through the communication network for an electronic-mail communication, and the transmission information is not encrypted prior to being transmitted through the communication network for a facsimile communication. By virtue of this feature, users of the claimed apparatus do not have to make arrangements for the different protocols for facsimile communications and electronic-mail communications, because the users merely have to operate a confidential button to maintain the confidentiality of transmission information in the communication network, thus improving the ease of operation when transmitting confidential information over the communication network.

Gordon relates to a messaging system that unifies voice mail, facsimile mail, and e-mail. As understood by Applicant, Gordon teaches that transmission information is encrypted at a UniPost Access Node 6 (see Fig. 1). Because the UniPost Access Node receives the transmission information through a public switched telephone network 10, which is a communication network, and subsequently encrypts the received transmission information, the security of the transmission information cannot be maintained until it is received at the UniPost

Access Node. Therefore, the Gordon system cannot provide as high a level of security to transmission information as the communication apparatus of Claim 1.

Nothing has been found in Gordon that is believed to teach or suggest a communication apparatus connected to a communication network, wherein the apparatus includes "input means for inputting transmission information to be transmitted to the destination apparatus designated by said destination designating means without using the communication network," and "encryption means for encrypting the transmission information inputted by said input means without using the communication network, wherein the transmission information is encrypted before being transmitted through the communication network to maintain confidentiality of the transmission information," and "security designating means for designating whether the transmission information is confidential or not according to an operation of a confidential button, wherein the confidential button is used when confidentiality of the transmission information is to be maintained," and "control means for controlling said facsimile communication means, said encryption means, and said electronic-mail means such that, if the transmission information has been designated as being confidential by said security designating means, said facsimile communication means transmits the inputted transmission information to the destination apparatus by facsimile transmission through the communication network, when said facsimile communication means has been designated by said communication designating means, and said electronic-mail communication means sends the encrypted transmission information to the destination apparatus by electronic mail through the communication network, when said electronic-mail communication means has been designated by said communication

designating means," as recited in Claim 1.

As mentioned above, Gordon is understood to teach away from inputting information without using a communication network, as claimed in Claim 1, because Gordon teaches that the UniPost Access Node receives transmission information through a communication network and subsequently encrypts the received transmission information. Therefore, unlike the communication apparatus of Claim 1, in the Gordon system the confidentiality of the transmission information may be breached before the UniPost Access Node receives it, because the transmission information is inputted to the UniPost Access Node via a communication network.

Further, Gordon is not seen to show or suggest the claimed security designating means, which designates whether transmission information is confidential or not according to an operation of a confidential button. The Office Action points to column 6, lines 28-33, of Gordon as disclosing security designating means "that makes a determination that the transmission information is confidential information when transmission by confidential communication is designated." Applicant respectfully traverses such a characterization of Gordon, and submits that the cited portion of Gordon merely states that "a file transfer from 22 to a facsimile machine of the subscriber can occur where the Toronto UniPost Access Node converts the communication to a facsimile communication and then forwards the communication to the particular facsimile machine. This type of communication conversion occurs transparently to the sender." Nothing in the cited portion relates to making a designation as to whether transmission information is confidential or not according to an operation of a confidential button. In fact, Gordon teaches

that the communication conversion is "transparent to the sender," which is understood to mean that the sender does not operate any confidential button, so therefore all communications are believed to undergo such a conversion. As such, Gordon is understood to teach away from designating whether transmission information is confidential or not according to an operation of a confidential button.

Should the Examiner disagree with the foregoing remarks, Applicant respectfully requests the Examiner to more particularly point out where and how Gordon discloses "security designation means for designating whether the transmission information is confidential or not according to an operation of a confidential button, wherein the confidential button is used when confidentiality of the transmission information is to be maintained," as claimed in Claim 1.

Accordingly, Applicant submits that Claim 1 is not anticipated by Gordon and respectfully requests withdrawal of the rejection under 35 U.S.C. § 102(b). Independent Claims 10 and 18 include a similar security designation feature as that discussed above, and therefore are believed to be patentable for at least the above reasons.

Yamada discloses a communication network that includes a telephone network and a LAN, but is not seen to remedy the deficiencies of Gordon. Therefore, Applicant respectfully submits that Claims 1-18 are patentable over Gordon and Yamada, considered individually or in combination.

The present Amendment After Final Action is believed clearly to place this application in condition for allowance. Therefore, its entry is believed proper under 37 C.F.R.

§ 1.116 and is respectfully requested, as an earnest effort to advance prosecution and reduce the number of issues. Should the Examincr believe that issues remain outstanding, it is respectfully requested that the Examiner contact Applicant's undersigned attorney in an effort to resolve such issues and advance the case to issue.

In view of the foregoing amendments and remarks, Applicant respectfully requests favorable reconsideration and early passage to issue of the present application.

No petition to extend the time for response to the Office Action is deemed necessary for the present Amendment. If, however, such a petition is required to make this Amendment timely filed, then this paper should be considered such a petition and the Commissioner is authorized to charge the requisite petition fee to Deposit Account 06-1205.

CONCLUSION

Applicant's undersigned attorney may be reached in our New York Office by telephone at (212) 218-2100. All correspondence should continue to be directed to our address listed below.

Respectfully submitted,

Attorney for Applicant
LOCK SEE for JAMES
Registration No. 38,667

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

NY_MAIN 390154v1